APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,315	01/17/2002	Edward M. Scheidt	STS 131 NP	4081

49691   7590   07/21/2005

IP STRATEGIES
12 1/2 WALL STREET
SUITE I
ASHEVILLE, NC 28801

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/936,315	SCHEIDT, EDWARD M.
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>06 June 2005</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>33-36</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>33-36</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) <u>1-31 and 37-41</u> are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>17 January 2002</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>8/9/2004</u>.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

1.   Applicant's election of <u>Group III</u> filed on 6/3/2005 with respect to restriction

requirement mailed on 5/4/2005 from the following three groups is acknowledged and

accordingly, this Office Action only addresses the claimed inventions of Group III as

elected by Applicant.

This application contains claims directed to the following patentably distinct

claimed inventions. Restriction to one of the following invention is required under 35

U.S.C 121:

   I.   Claims 1 – 28 drawn to particular key generator, classified in class 380,

           subclass 44.

   II.   Claims 29 – 32 and 37 – 41 drawn to specific data processing protection

           using cryptography, classified in class 713, subclass 189.

   III.   Claims 33 – 36 drawn to key management with respect to key distributed

           between two different parties without the distribution center, classified in

           class 380, subclass 283.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2.   Claim 33 and 35 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

This is because the claim limitation "generating, by the first party, a first asymmetric key pair based on the base, prime, and sub-prime parameters, and a shared key based on the second public key" is not clearly and specifically addressed in the specification. One skilled in the art clearly would not know how to use the claimed invention to make and use the same of the claimed invention.

Any other claims not addressed are rejected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly. claiming the subject matter which the applicant regards as his invention.

3.   Claim 33 and 35 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

Claim 33 and 35 are indefinite because the claim language "net label" is not

specifically defined in the specification and is therefore not clear what "net label" the

Applicant is exactly referred to as well as its exact usage.

Any other claims not addressed are rejected by virtue of their dependency should

also be corrected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claim 33 – 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Chen (Patent Number: 5796833), in view of Elgamal (Patent Number: 5657390).

As per claim 33 and 35, Chen teaches a method of establishing a secure

communication channel, comprising:

sending, by a first party, a secure call notification to a second party (Chen: Column 11 Line 40: session key protocol requires a connection (or call) request between two parties);

accessing, by the first and second parties, base, prime, and sub-prime parameters (Chen: Column 10 Line 41 – 47: the two prime numbers p and q are interpreted as prime and sub-prime to meet the claim language);

generating, by the second party, a second asymmetric key pair comprising a second public key and a second private key, based on the base, prime, and sub-prime parameters (Chen: Column 10 Line 41 – 47: the two prime numbers p and q are interpreted as prime and sub-prime to meet the claim language);

sending, by the second party to the first party, the second public key (Chen: Column 7 Line 59 – 60 and Column 11 Line 4 – 6);

generating, by the first party, a net label, a private label, a random value, a first asymmetric key pair comprising a first public key and a first private key based on the base, prime, and sub-prime parameters, and a shared key based on the second public key (Chen: Column 11 Line 20 – 25, Column 2 Line 59 – 60 and Column 7 Line 59 – 60: the common key is qualified as the shared key); However, Chen does not disclose expressly a generating net label, a private label, and a random value.

Elgamal teaches generating net label, a private label, and a random value (Elgamal: Column 7 Line 16 – 19: the challenge data is interpreted as a random value and associated set of data such as net label / private label, etc.).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Elgamal within the system of Chen

because (a) Chen discloses the needs of session key establishment protocol (Chen:

Column 11 Line 40 & Figure 2) and (b) Elgamal teaches a more efficient handshake

protocol associated with session key generation scheme (Elgamal: Column 2 Line 3 –

4).

encrypting, by the first party, the net label, the private label, and the random

value, using the shared key (Elgamal: Figure 6: the challenge data is encrypted by

server write key and besides the server write key and client write key is assume to be

the same as the shared key as taught by Chen);

sending, by the first party to the second party, the encrypted net label, the

encrypted private label, the encrypted random value, and the first public key (Elgamal:

Figure 6);

generating, by the second party, the shared key based on the first public key

Chen: Column 7 Line 59 – 60);

decrypting, by the second party, the encrypted net label, the encrypted private

label, and the encrypted random value using the shared key (Elgamal: Figure 6); and

exchanging, by the first and second parties, respective identification numbers to

establish the secure communication channel (Elgamal: Figure 6: This is the SSL

(Security Session Layer) communication channel as taught by Elgamal).

As per claim 34, Chen as modified further teaches the secure call notification is a first secure call notification, the .net label is a first net label, the private label is a first private label, the random value is a first random value, the shared key is a first shared key, the encrypted net label is a first encrypted first net label, the encrypted private label is a first encrypted first private label, and the encrypted random value is a first encrypted first random value further, the method further comprising:

designating, by one of the first party and the second party, either of the first party and the second party as a sender, and the other of the first party and the second party as a non-sender; suspending, by the sender, the secure communication channel between the first party and the second party; establishing, by the sender, a communication channel with a third party; sending, by the sender, a second secure call notification to the third party; accessing, by the third party, the base, prime, and sub-prime parameters; generating, by the third party, a third asymmetric key pair comprising a third private key and a third public key, based on the base, prime, and sub-prime parameters; sending, by the third party to the sender, the third public key; generating, by the sender, a second private label, a second net label, a second random value, a fourth asymmetric key pair comprising a fourth public key and a fourth private key based on the base, prime, and sub-prime parameters, and a second shared key based on the third public key; encrypting, by the sender, the second private label, the first net label, and the first random value, using the second shared key, to provide an encrypted second private label, a second encrypted first net label, and a second encrypted first random value; sending, by the sender to the third party, the encrypted

second private label, the second encrypted first net label, the second encrypted first

random value, and the fourth public key; generating, by the third party, the second

shared key based on the third public key; decrypting, by the third party, the encrypted

second private label, the second encrypted first net label, and the second encrypted first

random value, using the second shared key; suspending, by the sender, the secure

communication channel between the sender and the third party; sending, by the sender

to the third party and the non-sender, a conference call notification; encrypting, by the

sender, the second net label and the second random value, using one of the first public

key and the second public key, to provide a first encrypted second net label and a first

encrypted second random value; generating, by the sender, a first error detection value

for the first encrypted second net label and the first encrypted second random value;

sending, by the sender to the non-sender, the first encrypted second net label, the first

encrypted second random value, and the first error correction value; generating, by the

non-sender, a second error detection value, for the first encrypted second net label and

the first encrypted second random value; checking, by the non-sender, the validity of the

first encrypted second net label and the first encrypted second random value by

comparing the first and second error detection values; decrypting, by the non-sender,

the first encrypted second net label and the first encrypted second random value, using

one of the first private key and the second private key; encrypting, by the sender, the

second net label and the second random value, using the third public key, to provide a

second encrypted second net label and a second encrypted second random value;

generating, by the sender, a third error detection value, for the second encrypted

second net label and the second encrypted second random value; sending, by the

sender to the third party, the second encrypted second net label, the second encrypted

second random value, and the third error correction value; generating, by the third party,

a fourth error detection value, for the second encrypted second net label and the

second encrypted second random value; checking, by the third party, the validity of the

second encrypted second net label and the second encrypted second random value by

comparing the third and fourth error detection values; and decrypting, by the third party,

the second encrypted second net label and the second encrypted second random

value, using third private key (see the same rationale addressed above in rejecting the

claim 33 and 35).

As per claim 36, Chen as modified teaches deriving, by the first party, an error

checking code for each of the respective other parties from the respective encrypted net

labels and the respective encrypted random values (Chen: Column 1 Line 65 – 67,

Column 6 Line 38 – 49, Column 6 Line 59 – 65 and Column 7 Line 13 – 26: a hash

value is considered as an error checking code);

sending, by the first party, the respective error checking codes to the respective

other parties (Chen: Column 1 Line 65 – 67, Column 6 Line 38 – 49, Column 6 Line 59

– 65 and Column 7 Line 13 – 26); and

confirming, by the other parties, validity of the respective encrypted net

labels and the respective encrypted random values using the respective error checking

codes (Chen: Column 7 Line 13 – 26).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC
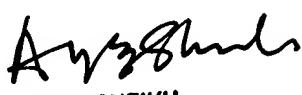
AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100